UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/783,214	02/15/2001	Sam Shiaw-Shiang Jiang	ASTP0010USA	2789

27765 7590 08/02/2004

NAIPO (NORTH AMERICA INTERNATIONAL PATENT OFFICE)
P.O. BOX 506
MERRIFIELD, VA 22116

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	6

DATE MAILED: 08/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

8

Office Action Summary	**Application No.** 09/783,214	**Applicant(s)** JIANG ET AL.	
	Examiner Longbit Chai	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _22 March 2002_.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-6_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _15 February 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _2_.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

2. The effective filing date for the subject matter defined in the pending claims in this application is 2/15/2001.

Specification

4. The abstract of the disclosure is objected to because the abstract paragraph exceeds 150 words (check for legalese, 1 paragraph, <150 words). Correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1 – 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Weinstein (Patent Number: 6094485), hereinafter referred to as Weinstein, in view of Chapman (Patent Number: 5926468), hereinafter referred to as Chapman, and in view of APA (Admitted Prior-Art), hereinafter referred to as APA.

4. As per claim 1, Weinstein teaches a method for performing a ciphering key change in a wireless communications system by resetting the sequence

number upon the ciphering key changes (Weinstein: see for example, Column 9 Line 29 – 34).

5. Weinstein does not expressly teach the detail synchronization mechanism of encryption engines at both ends especially between Layer 2 and Layer 3.

6. Chapman teaches the improved resynchronization mechanism of encryption engine between the Layer 2 and Layer 3 at both ends (even though not expressly for key change scenario) including a method, besides the reset of sequence number, that data link layer reset indication and acknowledgement can be carried in an information frame (I-Frame) rather than sending a reset command in a supervisory frame (S-Frame) so that overhead can be reduced and system bandwidth can be more efficiently utilized (Chapman: see for example, Column 7 Line 60 – 67, Column 68 Line 1 – 4, Column 2 Line 1 – 2, Column 2 Line 28 – 30, Column 2 Line 60 – 65, Column 5 Line 30 – 35, and Column 7 Line 47 – 50).

7. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Chapman within the system of Weinstein because Weinstein discloses resetting the sequence number on the event of ciphering key changes and Chapman further teaches the enhanced resynchronization mechanism between the Layer 2 data link layer and Layer 3 encryption engine as described above.

8. Therefore, Weinstein as modified teaches the resynchronization mechanism for encryption engines during the ciphering key changes between

both ends through resetting Layer 2 sequence number and improved Layer 2 reset command (and acknowledgement) without using Supervisory L2 Frame.

9. Weinstein as modified does not teach:

a. the first station executing a suspend function upon the signaling channel, the suspend function ensuring that the first station does not transmit PDUs to the second station along the signaling channel after a predetermined event.

10. However, this claim limitation can be rejected under the following two arguments explored below.

11. First Argument of Rejection:

12. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the enhanced data link reset mechanism to accommodate using the suspend function upon the signaling channel to assure the first station does not transmit PDUs to the second station because no further retransmission of ciphering reconfiguration command is assumed by the Applicant so that PDU transmission can be stopped until the reception of ACK message (as understood by the Examiner as Applicant expects; otherwise, the signaling channel can't be suspended prior to the reception of the ACK) – However, the transmission failure is extremely likely to occur in wireless applications especially when the transceivers operate in (or passes through) an inevitable transient fading environment. This is the reason Weinstein as modified does not expressly teach stop (or freeze) the sequence number during the transition period of ciphering key change by suspending the signaling channel transmission of PDU (Protocol Data Unit) and instead, Weinstein as modified

teaches resetting the sequence number as well as using data link reset indication / acknowledgement messages to synchronize the Layer 3 with Layer 2 to avoid running the sequence number past the event number where the new ciphering key would start getting used (Weinstein: see for example, Column 9 Line 29 – 34) & (Chapman: see for example, Column 7 Line 18 – 20).

13. Second Argument Rejection:

14. In addition to that, the modification would have been obvious because one of ordinary skill in the art would have been motivated to change the improved data link reset mechanism for encryption engine resynchronization to accommodate the suspension of PDU transmission because (a) both mechanisms do not start transmitting the enciphered information frame using the qualified sequence number in conjunction with the new ciphering key before the acknowledgement has been received in order to avoid running the sequence number past the event number (Chapman: see for example, Column 7 Line 18 – 20) & (Weinstein: see for example, Column 9 Line 29 – 34), (b) both ciphering engines intend to correspond the old ciphering key and new ciphering key to the enciphered information frames based on an event number. This event number used by the claim limitation is the sequence number suspended (or frozen) during the ciphering key change transition period while the event number taught by Chapman constitutes not only the reset sequence number (i.e. zero) but also the data link reset acknowledgement to assure the synchronization between the Layer 3 and Layer 2, and (c) both mechanisms would perform equally well because Chapman also teaches a method that data link layer reset indication

and acknowledgement can be carried in an information frame (I-Frame) rather than sending a reset command in a supervisory frame (S-Frame) so that overhead can be reduced and system bandwidth can be more efficiently utilized (Chapman: see for example, Column 2 Line 28 – 30 and Column 2 Line 1 – 2).

15. Weinstein as modified further teaches:

b. the first station transmitting the ciphering reconfiguration activation command along the signaling channel prior to the predetermined event (Weinstein: see for example, Column 9 Line 29 – 34).

c. the second station receiving the ciphering reconfiguration activation command and sending an acknowledgment to the first station (Weinstein: see for example, Column 9 Line 29 – 34).

d. the first station receiving the acknowledgment from the second station and canceling the suspend function so as to enable the first station to transmit PDUs to the second station along the signaling channel after the predetermined event (Same rationale applies herein in rejecting the claim limitation (a) as described as above).

e. wherein the first station and the second station use an old ciphering key prior to the predetermined event, and the first station and the second station use a new ciphering key after the predetermined event, the ciphering reconfiguration activation command informing the second station of the ciphering key change to the new ciphering key (Weinstein: see for example, Column 9 Line 29 – 34) & (Chapman: see for example, Column 7 Line 18 – 20).

16. Weinstein as modified teaches the wireless communication system comprising:

a. a first station capable of transmitting a ciphering reconfiguration activation command, the ciphering reconfiguration activation command being used to change a ciphering key (Weinstein: see for example, Column 9 Line 29 – 34) & (APA: see for example, Paragraph [0007]: Applicant's admitted prior art);

b. a second station capable of receiving the ciphering reconfiguration activation command and acknowledging reception of the ciphering reconfiguration activation command (Weinstein: see for example, Column 9 Line 29 – 34) & (APA: see for example, Paragraph [0007]: Applicant's admitted prior art);

17. Weinstein as modified does not teach the PDUs being at least partially enciphered using a ciphering key.

18. APA teaches:

c. wherein the first station and the second station are capable of establishing communications through at least a channel, the first station using a signaling channel to transmit the ciphering reconfiguration activation command, the first station and the second station utilizing layer 2 protocol data units (PDUs) to effect communications, the PDUs being at least partially enciphered using a ciphering key (APA: see for example, Paragraph [0004] Line 31 – 36 and Paragraph [0006] Line 25 – 28: Applicant's admitted prior art).

19. As per claim 2, Weinstein as modified teaches the claimed invention as described above (see claim 1). Weinstein as modified further teaches the ciphering reconfiguration activation command further informs the second station of the predetermined event so that the second station uses the new ciphering key after the predetermined event (Weinstein: see for example, Column 9 Line 29 – 34) & (APA: see for example, Paragraph [0007]: Applicant's admitted prior art).

20. As per claim 3, Weinstein as modified teaches the claimed invention as described above (see claim 1). Weinstein as modified further teaches the ciphering reconfiguration activation command is a layer 3 signaling message that is transmitted and received using layer 2 PDUs (Weinstein: see for example, Column 9 Line 29 – 34: SSL layer 3 signaling message is evidently built on top of Layer 2 PDU) & (APA: see for example, Paragraph [0004]: Applicant's admitted prior art).

21. As per claim 4, Weinstein as modified teaches the claimed invention as described above (see claim 1). Weinstein as modified further teaches the first station executing a suspend function upon every channel, each suspend function ensuring that the first station does not transmit PDUs to the second station along the corresponding channel after a corresponding predetermined event (See the same rationale addressed above in rejecting the claim 1).

22. As per claim 5, Weinstein as modified teaches the claimed invention as described above (see claim 4). Weinstein as modified further teaches the first station canceling the suspend function on each channel after receiving the acknowledgment from the second station so as to enable the first station to

transmit PDUs to the second station along each channel after the corresponding predetermined event (See the same rationale addressed above in rejecting the claim 1).

23. As per claim 6, Weinstein as modified teaches the claimed invention as described above (see claim 1). Weinstein as modified further teaches each PDU comprises a sequence number and the predetermined event is a suspend value; wherein when the suspend function is active, the first station will not transmit a PDU along the signaling channel to the second station if the PDU has a sequence number that is sequentially on or after the suspend value (See the same rationale addressed above in rejecting the claim 1).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100